# Tactical Information Operations and Effects Based Operations

# Outline

- Introductions
- References
- Purpose
- JRTC Trends
- Information Operations (IO) Overview
- IO and the MDMP
- Tactical Information Operations
- SOSO - Effects Based Operations

# Who We Are?

## LTC Kevin Milton

- BDE Fire Support O/C
- DIVARTY S3, BN S3, BDE FSO, 101st ABN Division (AASLT)
- Systems Integrator ODCOPS
- Battalion FSO, 1-160 (SOAR)
- Btry Commander, Battalion FSO, 101st ABN Division (AASLT)
- BMO, PLT LDR, & Btry FDO, 3rd Armored Division (Desert Storm)
- Contact Info:
  - kevin.milton@polk.army.mil
  - kevin-milton@us.army.mil
  - 337-531-8929 DSN 863-XXXX

## CW3 John P. Watson

- BDE TGT and Senior Radar O/C
- Counterfire Officer, 82d ABN Div
- Targeting Officer, 325th AIR
- 1st Armored Div
  - Counterfire Officer (SFOR 2/3)
  - Radar Tech (IFOR)
- Fire Direction (before the dark side)
- Contact Info:
  - jp.watson@us.army.mil
  - jp.watson@us.army.smil.mil
  - 337-531-9495 DSN 863-XXXX

# References

## Joint Pubs

- JP 3-08, Interagency Coordination During Joint Operations
- JP 3-13, Joint Doctrine for IO
- JP 3-60, Joint Doctrine for Targeting
- JP 5-00.1, Joint Doctrine for Campaign Planning
- JP 5-00.2, Joint Planning Guidance and Procedures

## Army Pubs

- FM 3-13, IO: Doctrine, and TTPs
- FM 3-60, TTP for Targeting
- FM 5-0, Staff Organization and Planning
- FM 3-0, Operations
- FM 3-90, Tactics
- FM 3-07, SOSO
- 1st IO CMC IO & MDMP TTP
- IO Planning Process Handbook

# Purpose

1. Familiarize you (quickly) with the lexicon and concepts of strategic and operational IO
2. Help you visualize offensive IO planning and execution requirements at the tactical level for SOSO.
3. Offer you some planning and tracking tools you can modify and apply when planning and executing tactical IO.

# You need to know….

1. 1st IO command is the successor to the Land Info Warfare Activity, and is the Army proponent for IO. FA 30 is the OPMS career field that supports IO.
2. To date, Army IO doctrinal products and training courses have focused at the strategic and operational level – it takes work to convert their tools to tactical use
3. There is no actual proponent for IO at BDE and below, and in many ways, at division level. We currently are the only CTC where tactical IO is currently taught, and due to our rotational structure its practical exercise is possible

# You also need to know….

**We have no complete solution to your problem (nor does anyone else), but using a combination of your experiences, existing doctrine, and our input you can find the right METT-TC solution to your specific tactical problem**

# Planting A Seed
## Behavior, Behavior, Behavior!

- The target audience's attitudes, feelings, cares, desires, etc are not the target of our IO campaign, they are instruments – strings we will play, to get the **BEHAVIOR** we want. A supportive attitude is useful and desirable, but it's not the be-all, end-all, and may be irrelevant.
- Example?
- In the end, we don't care how they feel about us, as long as the desired behavior is elicited.

# What We're Seeing and What We Provide To Train The Force?

# JRTC IO Trends

- Staffs are not building IO shaping operations into their COAs for combat ops or for SOSO.
- Units are uncomfortable/untrained in information operations.
- Prior to or during combat operations, brigade leadership often neglect to assign an IO Officer responsible for integrating IO into maneuver plans.

# JRTC Information Operations

- Past Combat rotations have incorporated IO in response to the JRTC environment.
  - COE Variables
    - Two/three different insurgent groups, each w/ different agenda
    - Terrorist and Criminal Organizations
      - Fully integrated enemy IO Campaign
      - Suicide bombings
      - Execution or murder of local officials
      - Remote detonating minefields, supported by hasty & deliberate ambush
  - Local Print Media & TV/Radio
  - Hostile/Neutral/Friendly Towns – up to 16 villages
- BCT and SFOR MREs IO experience
  - Language speakers
  - Ethnic role players
- OIF & OEF MRXs that replicate AOR campaign plans and current threats to the greatest extent possible.

# Information Operations Overview

**Everything we touch has become faster, more efficient, or otherwise improved by the information revolution.**

# Information Operations

Actions taken to affect adversary information and information systems while defending one's own information and information systems.

—Joint Publication 3-13

The employment of the core capabilities of electronic warfare, computer network operations, PSYOP, military deception, and operations security, in concert with specified supporting and related capabilities, to affect or defend information and information systems, and to influence decision-making.

—FM 3-13

# 14 ELEMENTS OF IO

**(PLUS 2 RELATED ACTIVITIES)**

## CORE ELEMENTS

- Operational Security (OPSEC)
- Psychological Operations (PSYOP)
- Military Deception
- Electronic Warfare (EW)
- Computer Network Operations
- Computer Network Attack
- Computer Network Defense
- Computer Network Exploitation

## SUPPORTING ELEMENTS

- Physical Destruction
- Information Assurance
- Physical Security
- Counterintelligence
- Counterdeception
- Counterpropaganda

## RELATED ACTIVITIES

- Civil Military Operations (CMO)
- Public Affairs (PA)

# 14 ELEMENTS OF IO

**(PLUS 2 RELATED ACTIVITIES)**

**CORE ELEMENTS**

- **Operational Security (OPSEC)**
- **Psychological Operations (PSYOP)**
- **Military Deception**
- **Electronic Warfare**
- **Computer Network Operations**
- **Computer Network Attack**
- **Computer Network Defense**
- **Computer Network Exploitation**

**These elements are used to plan both Offensive and Defensive Information Operations**

**SUPPORTING ELEMENTS**

- **Destruction**
- **Assurance**
- **Security**
- **Intelligence**
- **Deception**
- **Propaganda**

**RELATED ACTIVITIES**

- **Civil Affairs (CA)**
- **Public Affairs (PA)**

# IO Objectives for Offensive and Defensive IO Are Stated in Terms of EFFECTS

**Defensive IO**

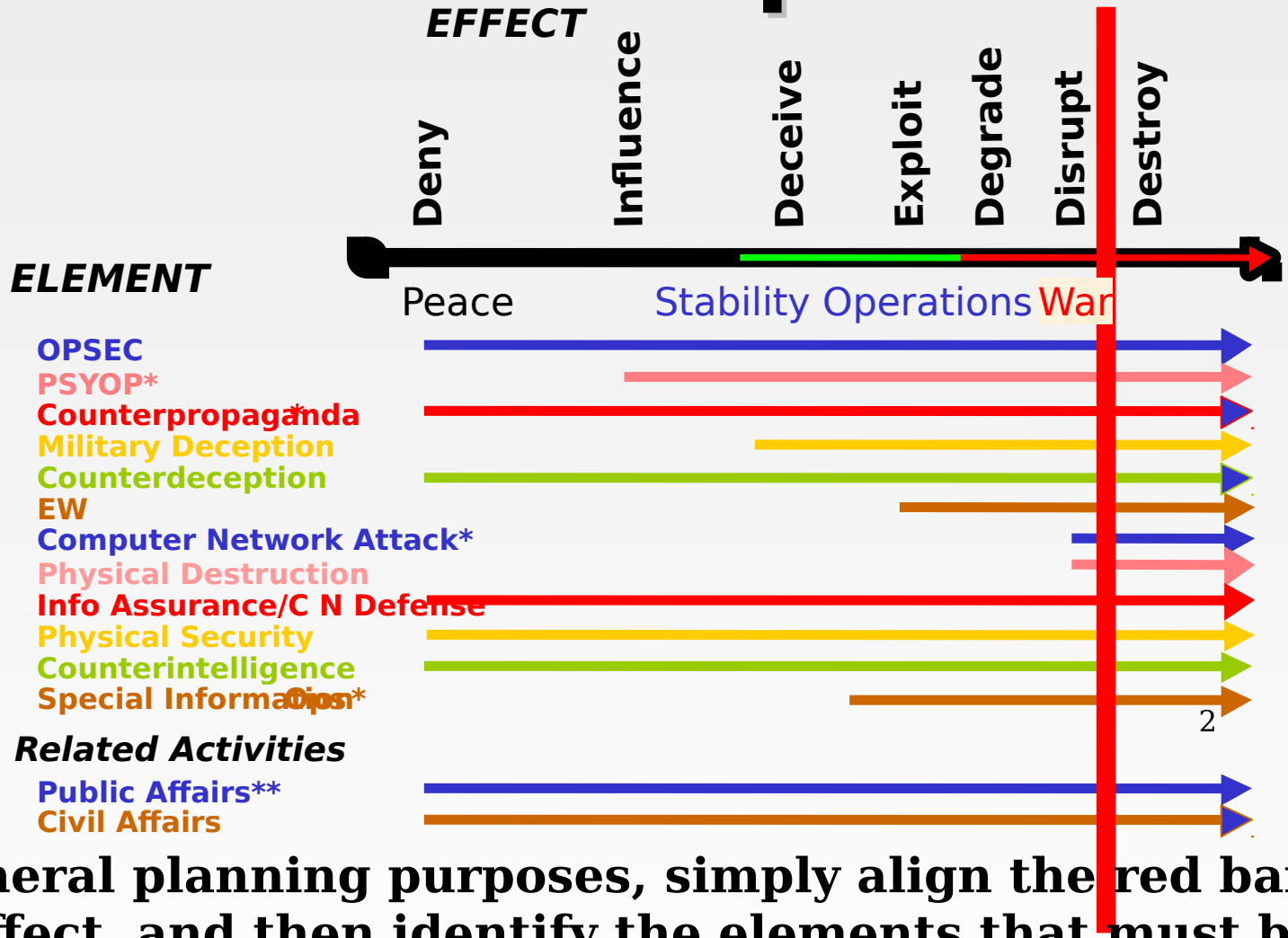
- Protect
- Detect
- Restore
- Respond

**Offensive IO**

- Destroy
- Degrade
- Disrupt
- Deny
- Deceive
- Exploit
- Influence

FM 3-13

# Information Operations




**For general planning purposes, simply align the red bar with desired effect, and then identify the elements that must be consi**

# Defensive Information Operations

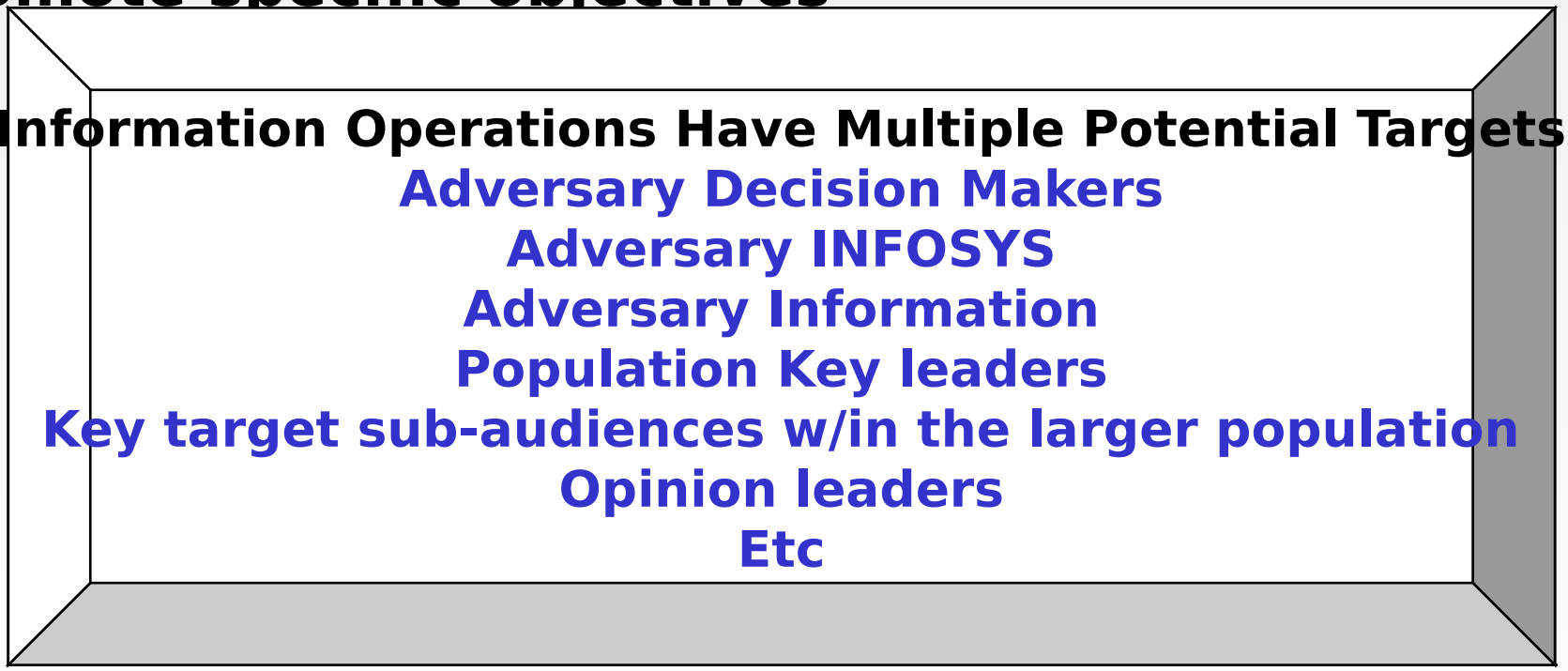
**The integration and coordination of policies and procedures, operations, personnel, and technology to protect and defend friendly information and information systems**

# Defensive IO Effects

- Protection: all actions taken to guard against or capture of sensitive equipment and information.
- Detection: to discover or discern the existence, presence, or fact of an intrusion into information systems.
- Restoration: to bring information systems back to their original state.
- Response: to react quickly to an adversary's information operations attack or intrusion.

# Offensive Information Operations

**The integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect enemy decision makers at all levels, or to influence others to achieve or promote specific objectives**



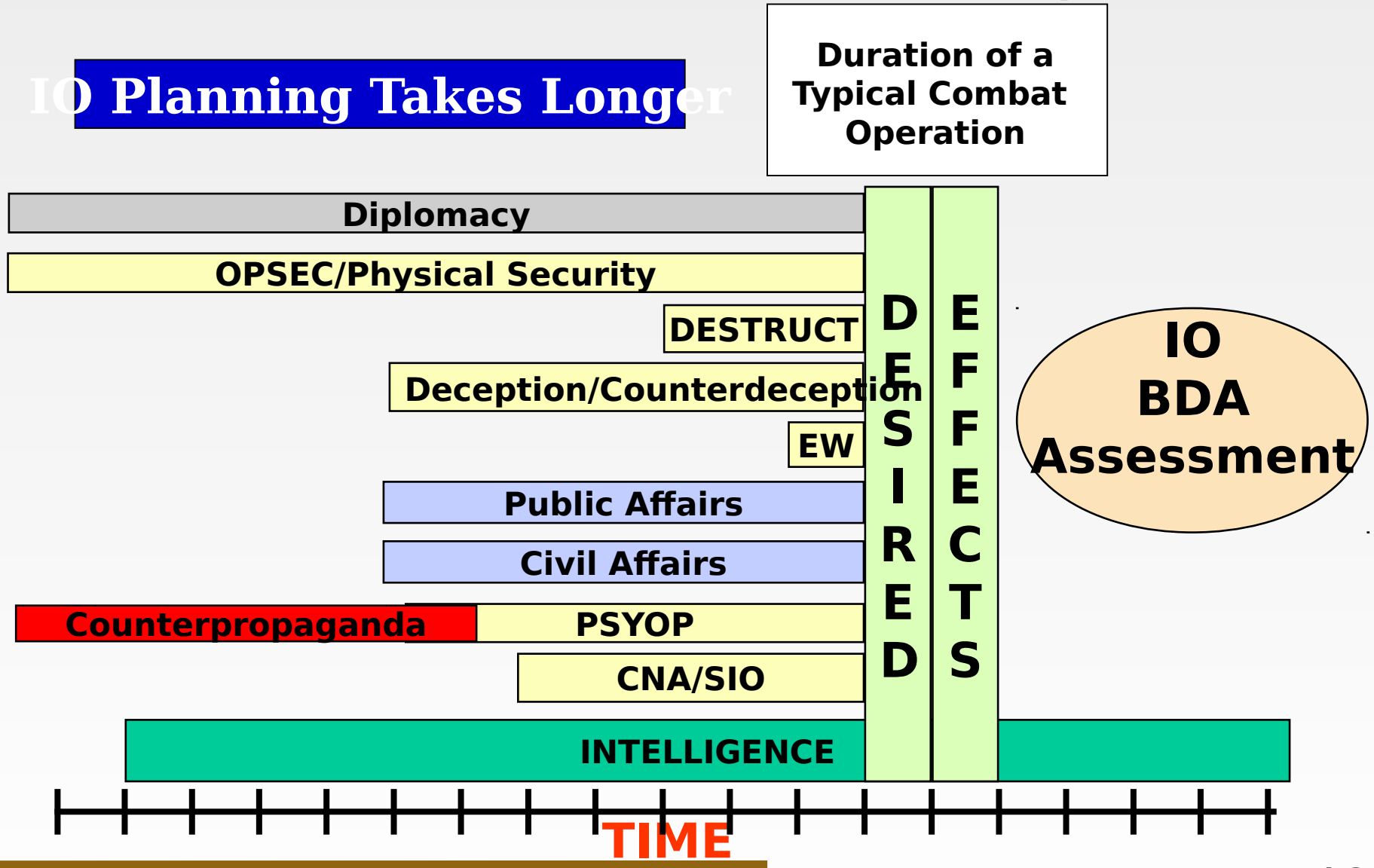
# Offensive IO Effects

- Destroy: to damage a combat system so badly that it cannot perform any function or be restored to a usable condition without being entirely rebuilt.
- Disrupt: in IO, means breaking or interrupting the flow of information between or interrupting the flow of information between selected C2 nodes.
- Degrade: in IO, is using non-lethal or temporary means to reduce the effectiveness or efficiency of adversary command and control systems, and information collection efforts or means.
- Deny: in IO, entails withholding information about Army force capabilities and intentions that adversaries need for effective and timely decision-making.
- Deceive: is to cause a person to believe what is not true.
- Exploit: in IO, is to gain access to adversary command and control systems to collect information or to plant false or misleading information.
- Influence:  to cause adversaries or others to behave in a manner favorable to Army forces.

# IO and the MDMP

# Developing and Synchronizing Effects Takes More Time To Plan And Execute Than Combat Operations

**IO Planning Takes Longer**



# Receipt of Mission

| MDMP Task | Information Sources (Inputs) | G-7 Actions | G-7 Products |
|---|---|---|---|
| Receipt of Mission | • Higher HQ OPLAN/ OPORD or deduced mission (figure B-2, page B-3)<br>• Commander's initial guidance (figure B-3, page B-5)<br>• IO estimate (appendix C) | • Participate in commander's initial assessment<br>• Receive the commander's initial guidance (figure B-3, page B-5)<br>• Perform an initial IO assessment<br>• Prepare for subsequent planning<br>• Allocate time to perform tasks | • Input to initial IPB, including initial EEFI (OPSEC)<br>• Input to initial ISR tasking (IO IRs); include IO IRs concerning adversary capability to collect EEFI (OPSEC)<br>• Submit IO IRs concerning adversary capability to collect EEFI to G-2 (OPSEC)<br>• IO input to first WARNO; input includes initial EEFI (figure B-4, page B-6)<br>• Recommend initial EEFI to G-2 & G-3 (OPSEC)<br>• Assemble DWG; begin MD mission analysis (MD)<br>• Update IO estimate<br>• Allocate available time |

# Mission Analysis (1 of 7)

| MDMP Task | Information Sources (Inputs) | G-7 Actions | G-7 Products |
|---|---|---|---|
| **Mission Analysis—** Analyze the Higher HQ Order | • Higher HQ OPLAN/OPORD, particularly the IO annex<br>• Commander's intent two echelons up<br>• Commander's initial IO guidance | • Understand higher commander's intent and concept of operations<br>• Understand higher commander's AO, mission-task constraints, acceptable risk, available assets<br>• Understand higher commander's schedule for conducting operations<br>• Understand missions of adjacent units<br>• Analyze the mission from an IO perspective<br>• Determine IO-related tasks assigned to the unit by higher HQ<br>• Identify information needed for IO planning | • IO-related tasks assigned to the unit by higher HQ |

# Mission Analysis (2 of 7)

| | | | |
|---|---|---|---|
| **Mission Analysis—Conduct IPB** | • Higher HQ IPB<br>• Higher HQ staff estimates<br>• Higher HQ OPLAN/OPORD | • Develop IO input to the IPB<br>• Analyze key friendly and adversary leaders and decisionmakers, supporting decisionmaking processes, INFOSYS, and C2 systems<br>• Identify adversary IO-related capabilities and vulnerabilities<br>• Analyze friendly IO capabilities and vulnerabilities<br>• Identify gaps in current intelligence on adversary IO<br>• Derive IO-related HPTs<br>• Describe the part of the information environment in the commander's battlespace and its effect on friendly and adversary IO<br>• Determine probable IO COAs<br>• Assess the potential effects of IO on adversary operations<br>• Determine additional EEFI (OPSEC) | • Provide IO input to IPB products. These become part of paragraph 2 of the IO estimate (figure B-5, page B-9)<br>• Submit IO IRs to G-2<br>• Nominations to HPTL for lethal and nonlethal attack (targeting)<br>• Refined EEFI (OPSEC) |

# Mission Analysis (3 of 7)

| MDMP Task | Information Sources (Inputs) | G-7 Actions | G-7 Products |
|---|---|---|---|
| **Mission Analysis—** Determine Specified, Implied, and Essential Tasks | • Specified and implied IO-related tasks from higher HQ OPLAN/OPORD<br>• IPB products | • Identify specified and implied IO-related tasks in the higher HQ OPLAN/OPORD.<br>• Develop IO-related implied tasks<br>• Determine additional EEFI (OPSEC)<br>• Develop IO input to the command targeting guidance<br>• Assemble critical asset list | • IO-related tasks (figure B-6, page B-11)<br>• Refined EEFI (OPSEC)<br>• Provide critical asset list to G-3 (figure B-6, page B-11)<br>• IO input to the command targeting guidance |
| **Mission Analysis—** Review Available Assets | • Current task organization (for IO assets)<br>• Higher HQ task organization (for IO resources)<br>• Status reports<br>• Unit SOP | • Identify friendly IO assets and resources<br>• Determine if available assets can perform all IO-related tasks<br>• Identify additional resources (such as fire support assets) needed to execute or support IO<br>• Compare available assets and resources to IO-related tasks | • List of available IO assets and capabilities (IO estimate paragraph 2c) (figure B-7, page B-12)<br>• Requests for additional IO resources, if necessary |

# Mission Analysis (4 of 7)

| MDMP Task | Information Sources (Inputs) | G-7 Actions | G-7 Products |
|---|---|---|---|
| **Mission Analysis— Determine Constraints** | • Commander's initial guidance<br>• Higher HQ OPLAN/OPORD | • Identify constraints (requirements and prohibitions) on IO, including those that affect possible OPSEC measures | • List of constraints on IO, including those that affect possible OPSEC measures (IO annex concept of support or coordinating instructions) (figure B-8, page B-13) |
| **Mission Analysis— Identify Critical Facts and Assumptions** | • Higher HQ OPLAN/OPORD<br>• Commander's initial guidance<br>• Observations and reports | • Identify facts and assumptions affecting IO elements<br>• Submit IO IRs for information that will confirm or disprove facts and assumptions<br>• Identify facts and assumptions that regarding OPSEC indicators that result in OPSEC vulnerabilities | • List of facts and assumptions pertinent to IO elements (IO estimate paragraph 2) (figure B-9, page B-13)<br>• IO IRs for information that will confirm or disprove facts and assumptions |
| **Mission Analysis— Conduct Risk Assessment** | • Higher HQ OPLAN/OPORD<br>• IPB<br>• Commander's initial guidance | • Identify and assess hazards associated with IO<br>• Identify OPSEC indicators<br>• Assess risk associated with OPSEC indicators to determine OPSEC vulnerabilities<br>• Establish provisional OPSEC measures | • List of assessed hazards to IO<br>• IO input to risk assessment (figure B-10, page B-14)<br>• List of provisional OPSEC measures |

# Mission Analysis (5 of 7)

| MDMP Task | Information Sources (Inputs) | G-7 Actions | G-7 Products |
|---|---|---|---|
| **Mission Analysis—Determine Initial CCIR** | • IO IRs | • Determine information the commander needs to make critical IO decisions or to assess IO actions<br>• Identify IO IRs to recommend as CCIR | • IO IRs nominated as CCIR (figure B-12, page B-16) |
| **Mission Analysis—Prepare the initial ISR Annex** | • Initial IPB<br>• PIRs/IO IRs | • Identify gaps in information needed to support IO planning and execution and assessment of early-initiation actions<br>• Confirm that the initial ISR annex includes IO IRs concerning adversary capability to collect EEFI | • IO IRs for information needed to support IO planning and execution and assessment of early-initiation actions<br>• IO IRs concerning adversary capability to collect EEFI |
| **Mission Analysis—Plan Use of Available Time** | • Revised G-3 time plan | • Determine time required to accomplish IO objectives<br>• Compare time available to accomplish essential IO-related tasks within the higher HQ time line and the adversary time line developed during IPB<br>• Refine initial time allocation plan | • IO time line (provided to G-3), with emphasis on the effect on IO of long lead-time events |

# Mission Analysis (6 of 7)

| MDMP Task | Information Sources (Inputs) | G-7 Actions | G-7 Products |
|---|---|---|---|
| **Mission Analysis—Write the Restated Mission** | • Initial IO mission<br>• Initial IO objectives | • Recommend possible IO objectives for inclusion in the restated mission | • IO-related essential tasks<br>• Restated IO mission<br>• IO objectives recommended for inclusion in the restated mission |
| **Mission Analysis—Conduct Mission Analysis Briefing** | • IO estimate<br>• Unit SOP | • Prepare to brief IO portion of mission analysis<br>• Brief MD estimate | • IO portion of mission analysis briefing (figure 5-4, page 5-18)<br>• MD estimate |
| **Mission Analysis—Approve the Restated Mission** | • Restated mission<br>• Mission analysis briefing | • Receive and understand the approved mission statement | • None |
| **Mission Analysis—Develop Initial Commander's Intent** | • Higher HQ commander's intent<br>• Results of mission analysis<br>• IO estimate | • Develop recommended IO input to the commander's intent | • Recommend IO input to the commander's intent (figure B-14, page B-17) |

# Mission Analysis (7 of 7)

| MDMP Task | Information Sources (Inputs) | G-7 Actions | G-7 Products |
|---|---|---|---|
| **Mission Analysis— Issue Commander's Guidance** | • Higher HQ OPLAN/OPORD<br>• Results of mission analysis<br>• IO estimate | • Develop recommended IO input to the commander's guidance<br>• Combine the refined EEFI with the provisional OPSEC measures to produce the OPSEC planning guidance | • Recommended IO input to the commander's guidance (figure B-15, page B-17)<br>• Recommended OPSEC planning guidance<br>• Recommended MD guidance<br>• Recommended IO targeting guidance |
| **Mission Analysis— Issue Warning Order** | • Commander's guidance and intent<br>• Approved restated mission, restated IO mission, and initial IO objectives<br>• IO mission analysis products | • Prepare input to the warning order. Input may include—<br>▪ Develop early taskings to subordinate units<br>▪ Initial IO mission statement<br>▪ OPSEC planning guidance<br>▪ Reconnaissance and surveillance taskings<br>▪ MD guidance | • Input to mission, commander's intent CCIR, and concept of operations (see figure B-16, page B-18)<br>• Recommend the initial IO mission statement |
| **Mission Analysis— Review Facts and Assumptions** | • Commander's guidance and intent<br>• Approved restated mission<br>• IO mission analysis products | • Review IO facts and assumptions<br>• Refine initial IO mission statement | • Updated facts and assumptions<br>• Refined IO mission statement<br>• Refined OPSEC measures |

# COA Development (1 of 4)

| MDMP Task | Information Sources (Inputs) | G-7 Actions | G-7 Products |
|---|---|---|---|
| COA Development—Analyze Relative Combat Power | • IPB<br>• Task organization<br>• IO estimate<br>• Vulnerability assessment | • Analyze IO effects on friendly and adversary capabilities, vulnerabilities, and combat power | • Description of the potential effect of IO on the relative combat power, stated by IO element |
| COA Development—Generate Options | • Commander's guidance and intent<br>• IPB<br>• Adversary and friendly IO assets, resources, and vulnerabilities | • Develop different ways for IO to support each COA<br>• Determine IO elements to use<br>• Determine how to focus IO on the overall objective<br>• Determine IO's role in the decisive and shaping operations of each COA<br>• Determine possible trade-offs between IO and other assets<br>• Develop MD COAs (deception stories) | • IO concept of support for each COA<br>• One or more MD COAs |

# COA Development (2 of 4)

| MDMP Task | Information Sources (Inputs) | G-7 Actions | G-7 Products |
|---|---|---|---|
| COA Development—Array Initial Forces | • Restated mission<br>• Commander's intent and guidance<br>• IPB<br>• MD plan or concept | • Allocate assets for each IO concept of support<br>• Identify requirements for additional IO resources<br>• Examine effect of possible MD COAs on force positioning<br>• Identify MD means | • Initial IO asset locations<br>• Additional IO resource requirements |
| COA Development—Develop Concept of Operations | • COAs (figure B-17, page B-22)<br>• IPB<br>• HVTL<br>• IO mission statement<br>• Initial IO concept of support for each COA | • For each COA—<br>• Develop IO concept of support (figures B-18, page B-24)<br>• Develop IO objectives<br>• Synchronize IO element actions<br>• Identify and prioritize offensive and defensive IO tasks<br>• Nominate selected HVTs as HPTs<br>• Determine initial IO task execution time line<br>• Refine IO input to risk assessment<br>• Develop IO assessment plan | • For each COA—<br>• IO input work sheet containing a refined IO concept of support, IO objectives, and IO tasks (figures B-19 through B-22, pages B-19–32)<br>• IO execution time line<br>• IO-related HPT nominations<br>• Critical asset list<br>• IO input to risk management plan, including residual risk associated with each OPSEC vulnerability (figure B-24, page B-34) |

# COA Development (3 of 4)

| MDMP Task | Information Sources (Inputs) | G-7 Actions | G-7 Products |
|---|---|---|---|
| | | • Identify additional EEFI<br>• Identify and assess OPSEC indicators to determine OPSEC vulnerabilities<br>• Develop OPSEC measures to shield OPSEC vulnerabilities<br>• Determine residual risk associated with each OPSEC vulnerability after OPSEC measures are applied (figure B-24, page B-34)<br>• Determine feedback required for assessment of MD COAs<br>• Conduct a risk assessment for each MD COA<br>• Conduct an OPSEC analysis for each MD COA<br>• Prepare termination branches for each MD COA | B-34)<br>• Criteria of success and IO IRs to support IO assessment<br>• Additional EEFI<br>• OPSEC vulnerabilities<br>• OPSEC measures (IO tasks) to shield OPSEC vulnerabilities |

# COA Development (4 of 4)

| MDMP Task | Information Sources (Inputs) | G-7 Actions | G-7 Products |
|---|---|---|---|
| COA Development—Recommend Headquarters | • IPB<br>• IO estimate<br>• IO vulnerability assessment<br>• IO tasks by IO element | • Assess C2 strengths and weaknesses to determine IO-related vulnerabilities of specific HQ<br>• Reevaluate critical asset list | • Recommendations concerning role of HQ in light of C2 vulnerability assessment<br>• Updated critical asset list<br>• Initial list of assets/re–sources to tasks assigned |
| COA Development—Prepare COA Statements and Sketches | • COA statement<br>• An IO concept of support and IO objectives for each COA | • Submit input for each COA statement/sketch to G-3<br>• Prepare IO concept of support statement and sketch for each COA | • Input for each COA statement/sketch<br>• IO concept of support sketches for each COA, stating the most important IO objectives |

# COA Analysis (1 of 2)

| MDMP Task | Information Sources (Inputs) | G-7 Actions | G-7 Products |
|---|---|---|---|
| COA Analysis | • COAs<br>• IPB<br>• IO input worksheets<br>• IO execution time line | • Develop evaluation criteria for each COA<br>• Synchronize IO tasks performed by different IO elements<br>• Integrate IO concept of support into the concept of operations for each COA<br>• Synchronize IO concept of support with that of higher and adjacent HQ<br>• Identify adversary IO capabilities and likely actions and reactions<br>• War-game friendly IO capabilities against adversary vulnerabilities<br>• War-game adversary IO capabilities against friendly vulnerabilities<br>• Synchronize and deconflict initial IO tasks<br>• Refine targeting guidance and HPTL<br>• Synchronize and deconflict IO targets<br>• Determine whether modifications to the COA result in additional EEFI or OPSEC vulnerabilities; if so, recommend OPSEC measures to shield them<br>• Assign attack measures to HPTs | • An evaluation of each MD COA in terms of criteria established before the war game<br>For each COA—<br>• An evaluation in terms of criteria established before the war game<br>• Refined IO input worksheets<br>• Refined IO concept of support<br>• Refined IO objectives<br>• Refined IO tasks<br>• Refined IO input to AGM and TSM<br>• IO IRs and RFIs identified during the war game<br>• Refined EEFI and OPSEC vulnerabilities, and OPSEC measures<br>• Paragraph 3 of the IO estimate<br>• IO input to G-3 synchronization matrix<br>• IO input to HPTL |

# COA Analysis (2 of 2)

| MDMP Task | Information Sources (Inputs) | G-7 Actions | G-7 Products |
|---|---|---|---|
| | | • Test OPSEC measures<br>• Determine decision points for executing OPSEC measures<br>• Determine operational support needed for OPSEC measures<br>• Determine OPSEC measures needed to support possible OPSEC branches and sequels<br>• Determine whether any OPSEC measures require addition coordination<br>• War-game each MD COA<br>• Identify each MD COA's potential branches; assess risk to the COA<br>• List the most dangerous/beneficial branch on IO decision support template or IO execution matrix | |

# COA Comparison

| MDMP Task | Information Sources (Inputs) | G-7 Actions | G-7 Products |
|---|---|---|---|
| COA Comparison | • COA evaluations from COA analysis<br>• COA evaluation criteria | • Compare the COAs with each other to determine the advantages and disadvantages of each<br>• Determine which COA is most supportable from an IO perspective<br>• Determine if any OPSEC measures require the commander's approval | • IO advantages and disadvantages for each COA<br>• Determine which COA is most supportable from an IO perspective<br>• IO COA decision matrix<br>• Paragraph 4, IO estimate |

# COA Approval & Order's Production

| MDMP Task | Information Sources (Inputs) | G-7 Actions | G-7 Products |
|---|---|---|---|
| COA Approval | • Results from COA comparison<br>• Recommended COA | • Provide IO input to COA recommendation<br>• Reevaluate IO input to the commander's guidance and intent<br>• Refine IO concept of support, IO objectives, and IO tasks for approved COA and develop associated IO execution matrix<br>• Prepare IO input to the WARNO<br>• Participate in COA decision briefing<br>• Recommend COA that IO can best support<br>• Request decision on executing any OPSEC measures that entail significant resource expenditure or risk | • Finalized IO concept of support for approved COA<br>• Finalized IO objectives and IO tasks based on approved COA<br>• IO input to WARNO (figure B-25, page B-36)<br>• IO execution matrix |
| Orders Production | • Approved COA<br>• Refined commander's guidance<br>• Refined commander's intent<br>• IO estimate<br>• IO execution matrix<br>• Finalized IO mission statement, IO concept of support, IO objectives, and IO tasks | • Ensures IO input (such as, EEFI and IO tasks to subordinate units) is placed in base OPLAN/OPORD<br>• Finalize IO annex<br>• Coordinate IO objectives and tasks (including OPSEC measures) with IO element staff officers<br>• Conduct other staff coordination<br>• Refine IO execution matrix | • IO synchronization matrix<br>• IO subparagraph to base OPLAN/ OPORD<br>• IO annex<br>• IO input to the AGM and TSM<br>• MD appendix to IO annex |